WHAT IS CLAIMED IS:

1. A security gateway for interfacing between virtual private network data packets and corporate network packets, each data packet comprising address information, the security gateway comprising:

a plurality of protocol modules each for processing packets in accordance with a different virtual private network protocol;

memory for storing sequence information identifying which of the protocol modules is to process each packet and the order of the processing;

a protocol discriminator for receiving data packets and being responsive to the address information of a received data packet for passing the received data packet to one or more of the protocol modules, for processing thereby in the sequence identified by the protocol sequence information.

2. A security gateway in accordance with claim 1 wherein each protocol module receiving a data packet passes the received packet back to the protocol discriminator upon completion of processing.

3. A security gateway in accordance with claim 2 wherein the protocol discriminator selectively sends a data packet received from one of the protocol modules to another of the protocol modules.

4. A security gateway in accordance with claim 3 comprising a firewall interface to a corporate network and the protocol discriminator passes data packets to the firewall interface after processing by one or more of the protocol modules.

5. A security gateway in accordance with claim 1 wherein one of the plurality of protocol modules processes virtual private network packets at a level 2

communication layer and another of the plurality of protocol modules processes virtual private network packets at a level 3 communication layer.

6. A security gateway in accordance with claim 5 wherein the one protocol module processes point-to-point tunneling protocol and layer 2 tunneling protocol.

7. A security gateway in accordance with claim 5 wherein the another protocol module processes packets in the IPSec protocol.

8. A security gateway in accordance with claim 1 comprising a packet filter responsive to address information in packets presented thereto for selectively granting and denying communication with the corporate network.

9. A security gateway in accordance with claim 8 comprising a stored table of access rules and the packet filter responds to the access rules for selectively granting and denying communication with the private network.

10. In a security gateway for interfacing between virtual private network packets and corporate network packets, each packet comprising address information and a plurality of protocol modules each for processing packets in accordance with a different virtual private network protocol, the method comprising:

storing protocol sequence information identifying which of the protocol modules is to process each packet and the order of the processing;

receiving data packets and responsive to addressing information of a received data packet, sending the received data packet to one or more of the protocol modules, for processing thereby in the sequence identified by the protocol sequence information.

11. A method in accordance with claim 10 comprising accumulating the protocol sequence information during authentication of one or more communication request packets.

12. A method in accordance with claim 10 comprising processing virtual private network packets at a level 2 communication layer in one of the plurality of protocol modules and processing virtual private network packets at a level 3 communication layer in another of the plurality of protocol modules.

13. A method in accordance with claim 10 comprising selectively granting and denying communication with the corporate network.

14. A method in accordance with claim 13 comprising storing a table of access rules upon which granting and denying communication with the private network is based.

15. A method of operating a security gateway in a virtual private network in which a user is assigned an IP address on a per session basis, the method comprising:

receiving at the security gateway a network packet and ascertaining from the packet the assigned IP address and the identity of the user initiating the packet;

identifying from storage at the security gateway rules and policies specifying permissions for the identified user to communicate and VPN protocols for packets from the identified user;

binding a portion of the rules and policies for the identified user to the assigned IP address of the user;

processing received packets in a plurality of protocol modules in accordance with the identified VPN protocols; and

controlling virtual packet network security

functions for packets from the user under direction of data in the rules and policies bound to the assigned IP address of the user.

16. A method in accordance with claim 15 wherein the rules and policies comprise data defining the security associations for communication between the user and the security gateway.

17. A method in accordance with claim 15 wherein the rules and policies comprise data for controlling access by the user to processes and data on a private network.

18. A method in accordance with claim 15 wherein the identifying step comprises negotiating VPN protocol attributes between the user and the security gateway.

241976 revised 12/14/00 khs:tgj